PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-288519
(43)Date of publication of application : 31.10.1995

(51)Int.Cl. H04L 9/06
H04L 9/14
G09C 1/00

(21)Application number : 06-080570
(22)Date of filing : 19.04.1994

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : YAMANAKA KIYOSHI
KANDA MASASUKI
KOYAIZU IKURO
TAKANO RIKUO

(54) DIGITAL INFORMATION COMMUNICATION SYSTEM AND ITS METHOD

(57)Abstract:
PURPOSE: To provide a digital information communication system preventing illegal use of information and its method and the digital information communication system in which an information utilizing terminal equipment is not limited and its method.
CONSTITUTION: The system is provided with a card section 1 having a security information storage section 11 storing a user identification number, a card secret key, a user signature key and a center verification key, and connects the card section 1 and a terminal equipment 2 when the terminal equipment 2 requests information from an information center equipment 3, and sends the user identification number stored in the card section 1 to the information center equipment 3 from the terminal equipment 2. Furthermore, the information itself received from the information center equipment 3 is ciphered by using the card secret key and the ciphered information is stored in the terminal equipment 2, the information itself is decoded by using the card secret key when the information itself is in use. Thus, the information is

utilized independently of the terminal equipment 2.

LEGAL STATUS

[Date of request for examination]	19.11.1999
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3276032
[Date of registration]	08.02.2002
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

CLAIMS

[Claim(s)]

[Claim 1] Voice, music, an image, and the enciphered digital information that consists of at least one of the alphabetic characters are received via a communication line from information centre equipment. In the digital information communication system used after accumulating this receipt information in a terminal unit, and decoding this receipt information While preparing the card section which has a security information are recording means to accumulate a user identification number, a card private key, a user signature key, and a center verification key, said terminal unit An interface means to connect said card section, and a communications control means to control the communication link between said information centre equipment, A verification means to verify the digital signature information received from said information centre equipment using said center verification key, A collating means to perform collating with the user identification

number accumulated in said card section, and the user identification number received from said information centre equipment, By input means to enter a password, session key extract means to extract the session key received from said information centre equipment using this password, and the public key cryptosystem By signature generation means to perform a digital signature using the user signature key accumulated in said card section to said session key, and the public key cryptosystem The signature information acquired by said signature generation means by open encryption means by which said center verification key performs encryption processing, and the conventional encryption system A common use encryption / decode means by which the card private key accumulated in said card section in the information received from said information centre equipment performs encryption/decode processing, It has an information output means to output to the format that the receipt information from said information centre equipment can be read and used. Said information centre equipment A communications control means to control the communication link between said terminal units, and a user information storage means to accumulate said user identification number corresponding to two or more registered users, a password, and a user verification key, By center signature key are recording means to accumulate the signature key of a center, session key generation means to generate the session key which enciphers a digital information body, and the public key cryptosystem By signature generation means by which said center signature key performs a digital signature to said session key, and the public key cryptosystem A decode means to perform decode processing of the encryption signature information received from said terminal unit, A verification means to verify the digital signature information acquired by this decode means using said user verification key, A signature information storage means to accumulate said digital signature information, and the session key received from said terminal unit, With a collating means to perform collating with the session key generated with said session key generation means, an information storage means to accumulate a digital information body, and a common key encryption system Digital information communication system characterized by having an encryption means to perform encryption processing of the digital information body set as the transmitting object within said information storage means using said session key.

[Claim 2] A card private key and a center verification key are digital information communication system according to claim 1 characterized by having two or more card sections which are the same values and have a user identification number and the value from which a user signature key

differs.

[Claim 3] Voice, music, an image, and the enciphered digital information that consists of at least one of the alphabetic characters are received via a communication line from information centre equipment. After accumulating this receipt information in a terminal unit, it is the digital information correspondence procedure used after decoding this receipt information. The card section which has a security information are recording means to accumulate a user identification number, a card private key, a user signature key, and a center verification key is prepared. In said terminal unit Digital information is required while transmitting the user identification number extracted from the security information are recording means of said card section to said information centre equipment. With information centre equipment The user identification number corresponding to two or more registered users, a password, and the password corresponding to the user identification number received from said terminal unit from a user information storage means by which the user verification key is accumulated are extracted. Subsequently After generating a session key and changing said user identification number, a password, and this session key with a secret function, It signs with the signature key which extracted this conversion result from the center signature key are recording means, and transmits to said terminal unit. In said terminal unit Verify the signature information received from said information centre with the center verification key extracted from the security information are recording means of said card section, and a user identification number is taken out. As compared with said transmitted user identification number, when this comparison result is an inequality, a circuit with said information centre equipment is cut. When said comparison result is coincidence, change said receipt information with a secret function, and a session key is extracted. After signing this session key with a user signature key, this signature information is enciphered with a center verification key, and it transmits to said information centre equipment. With information centre equipment After decoding the encryption signature information received from said terminal unit and accumulating signature information in a signature information storage means, The session key which verified this signature information with the user verification key, and extracted it, and said generated session key are collated. When said collating result is coincidence, after it cuts a circuit with said terminal unit when this collating result is an inequality, and said session key performs common use encryption for the information which had the demand from said terminal unit, Transmit to

said terminal unit and the session key received from said entered password and said information centre equipment is enciphered in a terminal unit with the card private key extracted from the security information are recording means of said card section. In case information is used with a terminal unit after accumulating in an information storage means with said received encryption digital information Said encryption password corresponding to information to use within said information storage means is decoded with the card private key extracted from the security information are recording means of said card section. Collate with the password entered from the input means, and informational use is forbidden when this collating result is an inequality. In coincidence, it is the digital information correspondence procedure characterized by decoding the information body enciphered with the session key which decoded the encryption session key with said card private key, and was obtained, and outputting from an information output means.

[Claim 4] Voice, music, an image, and the enciphered digital information that consists of at least one of the alphabetic characters are received via a communication line from information centre equipment. After accumulating this receipt information in a terminal unit, it is the digital information correspondence procedure used after decoding this receipt information. The card section which has a security information are recording means to accumulate a user identification number, a card private key, a user signature key, and a center verification key is prepared. The password enciphered with a registered user's user identification number, user verification key, and user verification key is accumulated in the user information storage means of said information centre equipment. In said terminal unit Digital information is required while transmitting the user identification number extracted from the security information are recording means of said card section to said information centre equipment. With information centre equipment The encryption password corresponding to the user identification number received from said terminal unit from said user information storage means is extracted. Subsequently After generating a session key and verifying with a user verification key, said user identification number, It signs with the signature key which extracted the encryption password and the encryption session key from the center signature key are recording means, and transmits to a terminal unit. In a terminal unit Verify the signature information received from said information centre equipment with the center verification key extracted from the security information are recording means of said card section, and a user

identification number is taken out. Furthermore, are comparing the encryption password, respectively and, in the case of a gap or an inequality, a circuit with said information centre equipment is cut. After a user identification number and a password sign the encryption session key received from said information centre equipment with a user signature key in coincidence, This signature information is enciphered with a center verification key, and it transmits to said information centre equipment. With information centre equipment After decoding the encryption signature information received from said terminal unit and accumulating signature information in a signature information storage means, The session key which verified this signature information with the user verification key, and extracted it, and said generated session key are collated. When said collating result is coincidence, after it cuts a circuit with said terminal unit when this collating result is an inequality, and said session key performs common use encryption for the information which had the demand from said terminal unit, Transmit to said terminal unit and the session key received from said entered password and said information centre equipment is enciphered in a terminal unit with the card private key extracted from the security information are recording means of said card section. In case information is used with a terminal unit after accumulating in an information storage means with said received encryption digital information Said encryption password corresponding to information to use within said information storage means is decoded with the card private key extracted from the security information are recording means of said card section. Collate with the password entered from the input means, and informational use is forbidden when this collating result is an inequality. In coincidence, it is the digital information correspondence procedure characterized by decoding the information body enciphered with the session key which decoded the encryption session key with said card private key, and was obtained, and outputting from an information output means.

[Claim 5] Voice, music, an image, and the enciphered digital information that consists of at least one of the alphabetic characters are received via a communication line from information centre equipment. After accumulating this receipt information in a terminal unit, it is the digital information correspondence procedure used after decoding this receipt information. The card section which has a security information are recording means to accumulate a user identification number, a card private key, a user signature key, and a center verification key is prepared. In a terminal unit Digital information is required while

transmitting the user identification number extracted from the security information are recording means of said card section to said information centre equipment. With said information centre equipment A random number is generated and it transmits to said terminal unit. In said terminal unit Verify the random number which signed with the user signature key and received the entered password from an encryption password and said information centre equipment further with a center verification key, and it transmits to said information centre equipment. With said information centre equipment, the encryption information received from said terminal unit is signed with a center signature key. Furthermore, the random number and password which verified the encryption password with the user verification key, and were obtained are collated with said transmitted random number and the password within a user information storage means, respectively. When either is an inequality, cut a circuit with said terminal unit, and in coincidence, a random number and a password generate a session key. This session key is enciphered with a user verification key, and it transmits to said terminal unit. In said terminal unit After signing the encryption session key received from said information centre equipment with a user signature key, this signature information is enciphered with a center verification key, and said information centre equipment is returned. With information centre equipment After decoding the encryption signature information received from said terminal unit and accumulating signature information in a signature information storage means, The session key which verified this signature information with the user verification key, and extracted it, and said generated session key are collated. When said collating result is coincidence, after it cuts a circuit with said terminal unit when this collating result is an inequality, and said session key performs common use encryption for the information which had the demand from said terminal unit, Transmit to said terminal unit and the session key received from said entered password and said information centre equipment is enciphered in a terminal unit with the card private key extracted from the security information are recording means of said card section. In case information is used with a terminal unit after accumulating in an information storage means with said received encryption digital information Said encryption password corresponding to information to use within said information storage means is decoded with the card private key extracted from the security information are recording means of said card section. Collate with the password entered from the input means, and informational use is forbidden when this collating result is an inequality. In coincidence, it is the digital

information correspondence procedure characterized by decoding the information body enciphered with the session key which decoded the encryption session key with said card private key, and was obtained, and outputting from an information output means.

[Claim 6] Voice, music, an image, and the enciphered digital information that consists of at least one of the alphabetic characters are received via a communication line from information centre equipment. After accumulating this receipt information in a terminal unit, it is the digital information correspondence procedure used after decoding this receipt information. The card section which has a security information are recording means to accumulate a user identification number, a card private key, a user signature key, and a center verification key is prepared. When said receipt information is used with a different terminal unit from the accepting-station equipment which received information, Connect with the information terminal unit which received said information from this use terminal unit, and a use terminal unit receives the encryption password corresponding to information to use from the information storage means of this information terminal unit. Information is decoded from information centre equipment with the card private key extracted from the card section used at the time of reception. Collate with the password entered with the input means of a use terminal unit, and information use is forbidden when this collating result is an inequality. In coincidence, the encryption session key corresponding to information to use is received from said information terminal unit. The digital information correspondence procedure characterized by receiving the enciphered information body using from said information terminal unit, decoding this information body with said session key in a use terminal unit, and outputting from an information output means after decoding with said card private key and obtaining a session key.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Industrial Application] In case this invention uses information after receiving and accumulating the information on the digital work enciphered [program / music, the image,] via a communication line, it

is easy to use it for a user, and it relates to the digital information communication system which took protection of copyright into consideration for the information provider, and its approach.
[0002]
[Description of the Prior Art] While changing works, such as music, an image, pictures, and books, into digital information in recent years by development of digital information compression technology (for example, MPEG=Moving Picture Image Coding Expert Group, KPEG=Joint Photographic Expert Group, etc.), such as voice, an animation, and a still picture, and the high-speed digital communication technique which makes ISDN representation, compression coding is carried out, and transmitting using a communication line is becoming realizable. Compared with digital information, such as an image, there is an example which is carrying out distribution service which already used personal computer communications etc. with computer software with little amount of data.
[0003] Since the conventional distribution channel is simplified by transmitting digital information using an ISDN communication line, it has the economical advantage which can carry out national delivery of the information quickly.
[0004]
[Problem(s) to be Solved by the Invention] However, when using the superior digital information which received by communication link use and was accumulated, the possibility of an unauthorized use of not only the normal user that received and purchased information but other users increases, and the problem which spoils the profits of a copyright person and an information provider arises by literary piracy. Moreover, if it was not usually in the installation of a terminal unit which received information for the normal user, there was a fault whose informational use becomes impossible.
[0005] The purpose of this invention is to offer the digital information communication system with which an informational use terminal is not limited to the digital information communication system which can prevent an informational unauthorized use and its approach, and a list, and its approach in view of the above-mentioned trouble.
[0006]
[Means for Solving the Problem] In order to attain the above-mentioned purpose, this invention in claim 1 Voice, music, an image, and the enciphered digital information that consists of at least one of the alphabetic characters are received via a communication line from information centre equipment. In the digital information communication system used after accumulating this receipt information in a terminal

unit, and decoding this receipt information While preparing the card section which has a security information are recording means to accumulate a user identification number, a card private key, a user signature key, and a center verification key, said terminal unit An interface means to connect said card section, and a communications control means to control the communication link between said information centre equipment, A verification means to verify the digital signature information received from said information centre equipment using said center verification key, A collating means to perform collating with the user identification number accumulated in said card section, and the user identification number received from said information centre equipment, By input means to enter a password, session key extract means to extract the session key received from said information centre equipment using this password, and the public key cryptosystem By signature generation means to perform a digital signature using the user signature key accumulated in said card section to said session key, and the public key cryptosystem The signature information acquired by said signature generation means by open encryption means by which said center verification key performs encryption processing, and the conventional encryption system A common use encryption / decode means by which the card private key accumulated in said card section in the information received from said information centre equipment performs encryption/decode processing, It has an information output means to output to the format that the receipt information from said information centre equipment can be read and used. Said information centre equipment A communications control means to control the communication link between said terminal units, and a user information storage means to accumulate said user identification number corresponding to two or more registered users, a password, and a user verification key, By center signature key are recording means to accumulate the signature key of a center, session key generation means to generate the session key which enciphers a digital information body, and the public key cryptosystem By signature generation means by which said center signature key performs a digital signature to said session key, and the public key cryptosystem A decode means to perform decode processing of the encryption signature information received from said terminal unit, A verification means to verify the digital signature information acquired by this decode means using said user verification key, A signature information storage means to accumulate said digital signature information, and the session key received from said terminal unit, With a collating means to perform collating with the session key generated with said session key

generation means, an information storage means to accumulate a digital information body, and a common key encryption system Digital information communication system equipped with an encryption means to perform encryption processing of the digital information body set as the transmitting object within said information storage means using said session key is proposed.

[0007] Moreover, in claim 2, in digital information communication system according to claim 1, a card private key and a center verification key are the same values, and propose the digital information communication system which has two or more card sections which have a user identification number and the value from which a user signature key differs.

[0008] Moreover, in claim 3, voice, music, an image, and the enciphered digital information that consists of at least one of the alphabetic characters are received via a communication line from information centre equipment. After accumulating this receipt information in a terminal unit, it is the digital information correspondence procedure used after decoding this receipt information. The card section which has a security information are recording means to accumulate a user identification number, a card private key, a user signature key, and a center verification key is prepared. In said terminal unit Digital information is required while transmitting the user identification number extracted from the security information are recording means of said card section to said information centre equipment. With information centre equipment The user identification number corresponding to two or more registered users, a password, and the password corresponding to the user identification number received from said terminal unit from a user information storage means by which the user verification key is accumulated are extracted. Subsequently After generating a session key and changing said user identification number, a password, and this session key with a secret function, It signs with the signature key which extracted this conversion result from the center signature key are recording means, and transmits to said terminal unit. In said terminal unit Verify the signature information received from said information centre with the center verification key extracted from the security information are recording means of said card section, and a user identification number is taken out. As compared with said transmitted user identification number, when this comparison result is an inequality, a circuit with said information centre equipment is cut. When said comparison result is coincidence, change said receipt information with a secret function, and a session key is extracted. After signing this

session key with a user signature key, this signature information is enciphered with a center verification key, and it transmits to said information centre equipment. With information centre equipment After decoding the encryption signature information received from said terminal unit and accumulating signature information in a signature information storage means, The session key which verified this signature information with the user verification key, and extracted it, and said generated session key are collated. When said collating result is coincidence, after it cuts a circuit with said terminal unit when this collating result is an inequality, and said session key performs common use encryption for the information which had the demand from said terminal unit, Transmit to said terminal unit and the session key received from said entered password and said information centre equipment is enciphered in a terminal unit with the card private key extracted from the security information are recording means of said card section. In case information is used with a terminal unit after accumulating in an information storage means with said received encryption digital information Said encryption password corresponding to information to use within said information storage means is decoded with the card private key extracted from the security information are recording means of said card section. Collate with the password entered from the input means, and informational use is forbidden when this collating result is an inequality. In coincidence, the digital information correspondence procedure which decodes the information body enciphered with the session key which decoded the encryption session key with said card private key, and was obtained, and is outputted from an information output means is proposed.

[0009] Moreover, in claim 4, voice, music, an image, and the enciphered digital information that consists of at least one of the alphabetic characters are received via a communication line from information centre equipment. After accumulating this receipt information in a terminal unit, it is the digital information correspondence procedure used after decoding this receipt information. The card section which has a security information are recording means to accumulate a user identification number, a card private key, a user signature key, and a center verification key is prepared. The password enciphered with a registered user's user identification number, user verification key, and user verification key is accumulated in the user information storage means of said information centre equipment. In said terminal unit Digital information is required while transmitting the user identification number extracted from the security information are recording means of

said card section to said information centre equipment. With information centre equipment The encryption password corresponding to the user identification number received from said terminal unit from said user information storage means is extracted. Subsequently After generating a session key and verifying with a user verification key, said user identification number, It signs with the signature key which extracted the encryption password and the encryption session key from the center signature key are recording means, and transmits to a terminal unit. In a terminal unit Verify the signature information received from said information centre equipment with the center verification key extracted from the security information are recording means of said card section, and a user identification number is taken out. Furthermore, are comparing the encryption password, respectively and, in the case of a gap or an inequality, a circuit with said information centre equipment is cut. After a user identification number and a password sign the encryption session key received from said information centre equipment with a user signature key in coincidence, This signature information is enciphered with a center verification key, and it transmits to said information centre equipment. With information centre equipment After decoding the encryption signature information received from said terminal unit and accumulating signature information in a signature information storage means, The session key which verified this signature information with the user verification key, and extracted it, and said generated session key are collated. When said collating result is coincidence, after it cuts a circuit with said terminal unit when this collating result is an inequality, and said session key performs common use encryption for the information which had the demand from said terminal unit, Transmit to said terminal unit and the session key received from said entered password and said information centre equipment is enciphered in a terminal unit with the card private key extracted from the security information are recording means of said card section. In case information is used with a terminal unit after accumulating in an information storage means with said received encryption digital information Said encryption password corresponding to information to use within said information storage means is decoded with the card private key extracted from the security information are recording means of said card section. Collate with the password entered from the input means, and informational use is forbidden when this collating result is an inequality. In coincidence, the digital information correspondence procedure which decodes the information body enciphered with the session key which decoded the encryption session key

with said card private key, and was obtained, and is outputted from an information output means is proposed.

[0010] Moreover, in claim 5, voice, music, an image, and the enciphered digital information that consists of at least one of the alphabetic characters are received via a communication line from information centre equipment. After accumulating this receipt information in a terminal unit, it is the digital information correspondence procedure used after decoding this receipt information. The card section which has a security information are recording means to accumulate a user identification number, a card private key, a user signature key, and a center verification key is prepared. In a terminal unit Digital information is required while transmitting the user identification number extracted from the security information are recording means of said card section to said information centre equipment. With said information centre equipment A random number is generated and it transmits to said terminal unit. In said terminal unit Verify the random number which signed with the user signature key and received the entered password from an encryption password and said information centre equipment further with a center verification key, and it transmits to said information centre equipment. With said information centre equipment, the encryption information received from said terminal unit is signed with a center signature key. Furthermore, the random number and password which verified the encryption password with the user verification key, and were obtained are collated with said transmitted random number and the password within a user information storage means, respectively. When either is an inequality, cut a circuit with said terminal unit, and in coincidence, a random number and a password generate a session key. This session key is enciphered with a user verification key, and it transmits to said terminal unit. In said terminal unit After signing the encryption session key received from said information centre equipment with a user signature key, this signature information is enciphered with a center verification key, and said information centre equipment is returned. With information centre equipment After decoding the encryption signature information received from said terminal unit and accumulating signature information in a signature information storage means, The session key which verified this signature information with the user verification key, and extracted it, and said generated session key are collated. When said collating result is coincidence, after it cuts a circuit with said terminal unit when this collating result is an inequality, and said session key performs common use encryption for the information which had the demand from said terminal unit, Transmit to

said terminal unit and the session key received from said entered password and said information centre equipment is enciphered in a terminal unit with the card private key extracted from the security information are recording means of said card section. In case information is used with a terminal unit after accumulating in an information storage means with said received encryption digital information Said encryption password corresponding to information to use within said information storage means is decoded with the card private key extracted from the security information are recording means of said card section. Collate with the password entered from the input means, and informational use is forbidden when this collating result is an inequality. In coincidence, the digital information correspondence procedure which decodes the information body enciphered with the session key which decoded the encryption session key with said card private key, and was obtained, and is outputted from an information output means is proposed.

[0011] Moreover, in claim 6, voice, music, an image, and the enciphered digital information that consists of at least one of the alphabetic characters are received via a communication line from information centre equipment. After accumulating this receipt information in a terminal unit, it is the digital information correspondence procedure used after decoding this receipt information. The card section which has a security information are recording means to accumulate a user identification number, a card private key, a user signature key, and a center verification key is prepared. When said receipt information is used with a different terminal unit from the accepting-station equipment which received information, Connect with the information terminal unit which received said information from this use terminal unit, and a use terminal unit receives the encryption password corresponding to information to use from the information storage means of this information terminal unit. Information is decoded from information centre equipment with the card private key extracted from the card section used at the time of reception. Collate with the password entered with the input means of a use terminal unit, and information use is forbidden when this collating result is an inequality. In coincidence, the encryption session key corresponding to information to use is received from said information terminal unit. After decoding with said card private key and obtaining a session key, the enciphered information body to use from said information terminal unit is received, and the digital information correspondence procedure which decodes this information body with said session key in a use terminal unit, and is

outputted from an information output means is proposed.

[0012]

[Function] According to claim 1 of this invention, a user identification number, a card private key, a user signature key, and a center verification key are accumulated in the security information are recording means of the card section. Moreover, in case transfer of the information between a terminal unit and information centre equipment is performed by the communications control means formed in each and information is required of said information centre equipment from said terminal unit, said terminal unit and said card section are connected through an interface means, and the user identification number accumulated in the security information are recording means of said card section is transmitted to said information centre equipment. While the password corresponding to this user identification number was searched with the information centre equipment which received said user identification number from the user information-storage means, after the session key which enciphers a digital-information body with a session key generation means is generated, it is signed by the signature generation means to this session key, a user identification number, and a password using the center signature key accumulated in the center signature key are-recording means, and it is transmitted to said terminal unit. In the terminal unit which received this signature information, by the verification means, said signature information is verified using the center verification key accumulated in the security information are recording means of said card section, and a user identification number is taken out from this signature information. Subsequently, when collating with this identification number and the user identification number accumulated in said card section is performed and these user identification numbers are in agreement with a collating means as a result of this collating, said session key is extracted from said signature information by the session key extract means using the password entered from the input means. Then, while a signature is made by the signature generation means as a check which received the session key using the user signature key accumulated in said card section to this session key, it is enciphered by the open encryption means with a center verification key, and is transmitted to said information centre equipment by it. With the information centre equipment which received this encryption signature information, by the decode means, this encryption signature information is decoded and it is accumulated in a signature information storage means. Furthermore, while this signature information is verified by the verification means with the user

verification key accumulated in the user information storage means Collating with the session key received from said terminal unit with the collating means and the session key generated by said session key generation means is performed. When these are in agreement as a result of this collating, after the information body which had the demand from said terminal unit is taken out from an information storage means and encryption processing is performed by the encryption means, it is transmitted to said terminal unit. While the session key received in the terminal unit which received the demanded information body from the password entered by common-use encryption / decode means and information centre equipment is enciphered with said card private key, in case it is accumulated with the received encryption digital-information body and this information body uses, said information body is read, and it is changed and outputted by the information output means to the format which can use.

[0013] Moreover, according to claim 2, a card private key and a center verification key are the same values, and two or more card sections which have the value from which a user identification number and a user signature key differ are prepared in digital information communication system. The information which those who own by this the card section a card private key and whose center verification key are the same values demanded becomes usable [other persons who own the card section which has the card private key and center verification key of the same value].

[0014] Moreover, digital information is required while the user identification number extracted from the terminal unit from the security information are recording means of the card section is transmitted to information centre equipment according to claim 3. The user identification number corresponding to two or more registered users [equipment / which received this demand / information centre], A password and the password corresponding to the user identification number received from said terminal unit from a user information storage means by which the user verification key is accumulated are extracted. Subsequently After a session key is generated and said user identification number, a password, and this session key are changed with a secret function, this conversion result is signed using the signature key extracted from the center signature key are recording means, and is transmitted to said terminal unit. In the terminal unit which received this signature information, the signature information received from said information centre It is verified with the center verification key extracted from the security information are recording means of said card section, and a user identification number is taken out. Are compared

with said transmitted user identification number, and when this comparison result is an inequality, a circuit with said information centre equipment is cut. When said comparison result is coincidence, this signature information is enciphered with a center verification key, and said receipt information is transmitted to said information centre equipment, after being changed with a secret function, extracting a session key and signing this session key with a user signature key. With this information centre equipment that carried out encryption signature information reception After the encryption signature information received from said terminal unit was decoded and this signature information was accumulated in the signature information storage means, The session key which verified this signature information with the user verification key, and extracted it, and said generated session key are collated. When this collating result is an inequality, a circuit with said terminal unit is cut, and when said collating result is coincidence, after common use encryption of the information which had the demand from said terminal unit is carried out with said session key, it is transmitted to said terminal unit. In a terminal unit, then, the session key received from said entered password and said information centre equipment It is enciphered with the card private key extracted from the security information are recording means of said card section. In case it is accumulated in an information storage means with said received encryption digital information and information is used with a terminal unit Said encryption password corresponding to information to use within said information storage means It decodes with the card private key extracted from the security information are recording means of said card section. It collates with the password entered from the input means, when this collating result is an inequality, informational use is forbidden, and when it is coincidence, the information body enciphered with the session key which decoded the encryption session key with said card private key, and was obtained is decoded, and it is outputted from an information output means.

[0015] Moreover, according to claim 4, the password enciphered with a registered user's user identification number, user verification key, and user verification key is accumulated in the user information storage means of information centre equipment, and a terminal unit requires digital information, while the user identification number extracted from the security information are recording means of said card section is transmitted to said information centre equipment. The encryption password corresponding to the user identification number received from said terminal unit from said user information-storage means is extracted,

and after a session key is generated and being verified with a user verification key, it is signed with the signature key extracted from the center signature key are-recording means to said user identification number, the encryption password, and the encryption session key, and, subsequently it is transmitted to said terminal unit with the information centre equipment which received the demand of information from said terminal unit. In the terminal unit which received this signature information, the signature information received from said information centre equipment It is verified with the center verification key extracted from the card section security information are recording means, and a user identification number is taken out. Furthermore, the encryption password is compared, respectively and, in the case of a gap or an inequality, a circuit with said information centre equipment is cut. After the encryption session key which received the user identification number and the password from said information centre equipment in coincidence is signed with a user signature key, it is enciphered with a center verification key and this signature information is transmitted to said information centre equipment. With the information centre equipment which received this encryption signature information After the encryption signature information received from said terminal unit was decoded and signature information was accumulated in the signature information storage means, The session key which verified this signature information with the user verification key, and extracted it, and said generated session key are collated. When this collating result is an inequality, a circuit with said terminal unit is cut, and when said collating result is coincidence, after common use encryption of the information which had the demand from said terminal unit is carried out with said session key, it is transmitted to said terminal unit. In said terminal unit, then, the session key received from said entered password and said information centre equipment It is enciphered with the card private key extracted from the security information are recording means of said card section. In case it is accumulated in an information storage means with said received encryption digital information and information is used with a terminal unit Said encryption password corresponding to information to use within said information storage means It decodes with the card private key extracted from the security information are recording means of said card section. It collates with the password entered from the input means, when this collating result is an inequality, informational use is forbidden, and when it is coincidence, the information body enciphered with the session key which decoded the encryption session key with said

card private key, and was obtained is decoded, and it is outputted from an information output means.

[0016] Moreover, according to claim 5, in the case of information requirements, while the user identification number extracted from the security information are recording means of the card section is transmitted to information centre equipment, digital information is required, and a random number is generated and it is transmitted to said terminal unit with a terminal unit with the information centre equipment which received this demand. In the terminal unit which received this random number, the entered password is signed with a user signature key, and the random number further received from an encryption password and said information centre equipment is verified with a center verification key, and is transmitted to said information centre equipment. Then, with said information centre equipment, the encryption information received from said terminal unit is signed with a center signature key. Furthermore, the random number and password which were verified and obtained with the user verification key an encryption password It collates with said transmitted random number and the password within a user information storage means, respectively. In coincidence of a random number and a password, when either is an inequality, a circuit with said terminal unit is cut, and a session key is generated, and this session key is enciphered with a user verification key, and it is transmitted to said terminal unit. Subsequently, in said terminal unit, after the encryption session key received from said information centre equipment is signed with a user signature key, this signature information is enciphered with a center verification key, and said information centre equipment is returned. Furthermore, with information centre equipment, the encryption signature information received from said terminal unit is decoded. After signature information is accumulated in a signature information storage means, the session key which verified this signature information with the user verification key, and extracted it, and said generated session key are collated. When this collating result is an inequality, a circuit with said terminal unit is cut, and when said collating result is coincidence, after common use encryption of the information which had the demand from said terminal unit is carried out with said session key, it is transmitted to said terminal unit. In a terminal unit, then, the session key received from said entered password and said information centre equipment It is enciphered with the card private key extracted from the security information are recording means of said card section. In case it is accumulated in an information storage means with said received encryption digital information and

information is used with a terminal unit Said encryption password corresponding to information to use within said information storage means It decodes with the card private key extracted from the security information are recording means of said card section. It collates with the password entered from the input means, when this collating result is an inequality, informational use is forbidden, and when it is coincidence, the information body enciphered with the session key which decoded the encryption session key with said card private key, and was obtained is decoded, and it is outputted from an information output means.

[0017] moreover, in case said receipt information is used with a different terminal unit from the accepting-station equipment which received information according to claim 6 This use terminal unit is connected to the information terminal unit which received said information, and the encryption password corresponding to information to use from the information storage means of this information terminal unit is received by the use terminal unit. It decodes with the card private key extracted from the card section used at the time of the information reception from information centre equipment, and the this decoded password and the password entered by the input means of a use terminal unit are collated, and information use is forbidden when this collating result is an inequality. Moreover, when a collating result is coincidence, after receiving the encryption session key corresponding to information to use for said use terminal unit from said information terminal unit, decoding with said card private key and obtaining a session key, the enciphered information body to use from said information terminal unit is received, and this information body is decoded with said session key in a use terminal unit, and is outputted from an information output means.

[0018]

[Example] Hereafter, one example of this invention is explained based on a drawing. Drawing 1 is the block diagram showing the 1st example of this invention. In drawing, 1 is the card section and it is possible to use the card which is equipped with the security information are recording section 11 which accumulates a user identification number, a card private key, a user signature key, and a center verification key, for example, consists of a magnetic card, an IC card, and an optical storage.

[0019] 2 is a terminal unit. The communication link between the information centre equipment mentioned later The communications control section 20 to control, the verification section 21 which verifies the

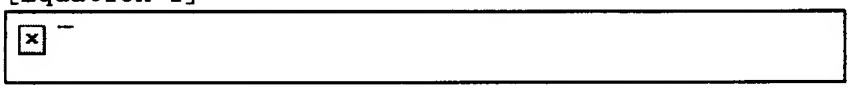
digital signature information from information centre equipment, the collating section 22 which performs collating of the contents of information, the input section 23 which enters a password, the session key extract section 24 which extracts the session key received from information centre equipment, By the signature generation section 25 and the public key cryptosystem which perform a digital signature by the public key cryptosystem It has the open encryption section 26 which performs encryption processing, common use encryption / decode section 27 which performs encryption/decode processing by the conventional encryption system, the information storage section 28 which accumulates receipt information, and the information output section 29 come out of and made into the format that receipt information can be read and used.
[0020] The communications control section 30 which 3 is information centre equipment and controls the communication link between terminal units 2, said user identification number corresponding to two or more registered users, A password, With the user information storage section 31 which accumulates a user verification key, the center signature key are recording section 32 which accumulates the signature key of a center, the session key generation section 33 which generates the session key which enciphers a digital information body, and a public key crypto system By the signature generation section 34 and the public key cryptosystem which perform a digital signature With the decode section 35 which performs decode processing, the verification section 36 which verifies the digital signature information from a terminal unit 2, the signature information storage section 37 which accumulates said digital signature information, the collating section 38 which performs collating of the contents of information, and a common key encryption system It has the encryption section 39 which performs encryption processing, and the information storage section 40 which accumulates a digital information body.
[0021] Next, reception of the information in the digital information communication system of the 1st example which consists of the above-mentioned configuration, and the operations sequence to are recording are explained based on the flow chart shown in drawing 2 . First, the card section 1 of the user who wants to use information is connected to a terminal unit 2. A connection method can insert the card section 1 in the slot for card insertion of a terminal unit 2, or can respond variously by the physical configuration and functions of the card section 1 and a terminal unit 2, such as connection by wireless, such as a cable cable or infrared radiation, and an electric wave.
[0022] Subsequently, a terminal unit 2 is connected to information

centre equipment 3 through a communication line, the user identification number UIDi extracted from the security information are recording section 11 of the card section 1 is transmitted, and the contents of digital information are required (SA1). The contents of information of the security information are recording section 11 of the card section 1 are shown in drawing 3 . The user identification number UIDi, the card private key Ki, the user signature key Di, and the center verification key Cp are accumulated in the security information are recording section 11 of the card section 1.

[0023] The password PWi corresponding to said user identification number UIDi received from the terminal unit 2 is searched with information centre equipment 3 from the user information storage section 31 (SA2). The contents of information of the user information storage section 31 are shown in drawing 4 . Corresponding to this, Password PWi and the user verification key Ei are accumulated in the user information storage section 31 at the user identification number UIDi and the list.

[0024] Subsequently, it is the session key Session for encryption of an information body at the session key generation section 33 of information centre equipment 3. It generates (SA3). Session key Session There are various approaches, such as generation by random number generation, and a generation method can also use which approach. Then, generated session key Session And after changing said user identification number UIDi and Password PWi which were searched with a specific secret function (SA4), in the signature generation section 34, it signs with the signature key Cs which extracted this conversion result by the center signature key are recording section 32 (SA5), and transmits to a terminal unit 2 (SA6). The contents of information of the center signature key are recording section 32 are shown in drawing 5 . Here, a secret function is a function which only a terminal unit 2 and information centre equipment 3 know, and is a function which is not told to a user. For example, the secret function f is the following (1). It is expressed by the formula.

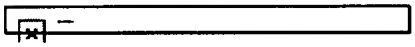
[Equation 1]



Moreover, a signature is the following (2) here. As shown in a formula, it says decoding with the private key (signature key) Cs of information centre equipment 3 by the public key cryptosystem.

[0025]

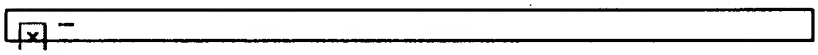
[Equation 2]



In a terminal unit 2, in the verification section 21, said received signature information is verified with the center verification key Cp extracted from the security information are recording section 11 of the card section 1, and a user identification number is taken out (SA7). Here, verification is the following (3). As shown in a formula, it says enciphering with the public key (verification key) Cp of the information centre equipment 3 by the public key cryptosystem.

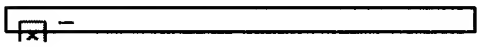
[0026]

[Equation 3]



Then, by the collating section 22, said taken-out user identification number is compared with a terminal unit 2 to said transmitted user identification number (SA8), and when this comparison result is an inequality, a circuit with information centre equipment 3 is cut (SA9). Moreover, when the comparison result of said SA8 is coincidence, by the session key extract section 24, inverse transformation is carried out to having used it with information centre equipment 3 from said receipt information with the same secret function, and a session key is extracted (SA10).

[0027] At the example of the secret function mentioned above, it is the following (4). Since a formula is realized, it is [Equation 4].

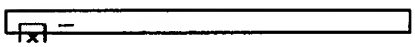


A session key is obtained by entering a password from the input section 23 and searching for the exclusive OR of the output of this password and the verification section 21.

[0028] Next, a terminal unit 2 is the following (5) as a check which received the session key. As shown in a formula Session key Session received by the signature generation section 25 While signing with the user signature key Di extracted from the security information are recording section 11 of the card section 1 (SA11), by the open encryption section 26 This signature information is enciphered with the center verification key Cp (SA12), and it transmits to information centre equipment 3 (SA13).

[0029]

[Equation 5]

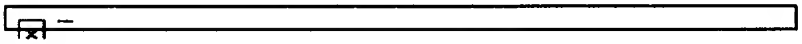


Then, with information centre equipment 3, it is the following (6) by

the decode section 35. As shown in a formula, said received encryption signature information is decoded using the center signature key Cs (SA14), and the decoded signature information is accumulated in the signature information storage section 37 (SA15).

[0030]

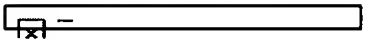
[Equation 6]



While information centre equipment 3 verifies this signature information with the user verification key Ei in the user information storage section 31 (SA16), by the verification section 36 next, by the collating section 38 The extracted session key and said generated session key are collated (SA17). When this collating result is an inequality, a circuit with a terminal unit 2 is cut (SA18), and the information which had the demand from the terminal unit 2 in coincidence is taken out from the information storage section 40. By the encryption section 39 The following (7) As shown in a formula, it is said session key Session. It uses, common use encryption is performed (SA19), and it transmits to a terminal unit 2 (SA20).

[0031]

[Equation 7]



With a terminal unit 2, they are said entered password PWi and said received session key Session by common use encryption / decode section 27. It enciphers using the card private key Ki extracted from the security information are recording section 11 of the card section 1 (SA21), and accumulates in the information storage section 28 with said received encryption digital information (SA22). It is the session key Session to Password PWi and the session key Session which were enciphered using the card private key Ki as shown in the information storage section 28 at drawing 6 , and a list. The information body used and enciphered is accumulated.

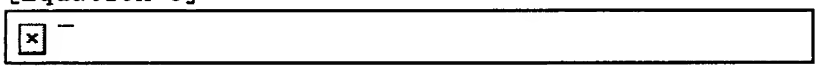
[0032] In addition, after in the case of the inequality in user identification number collating in the terminal unit 2 shown in drawing 2 , and session key collating in information centre equipment 3 repeating reinput of the count of assignment, and retransmission of message rather than cutting ******, you may make it cut a circuit.

[0033] Next, in the digital information communication system of the 1st example, the procedure in the case of using the received information with a terminal unit 2 is explained based on the flow chart shown in

drawing 7 .
[0034] In case the information received from information centre equipment 3 in the terminal unit 2 is used, while extracting said encryption password PWi corresponding to information to use in the information accumulated in the information-storage section 28 of a terminal unit 2 (SB1), said extracted encryption password PWi decodes by common-use encryption / decode section 27 using the card private key Ki extracted from the security-information are-recording section 11 of the card section 1 (SB2). Then, the compounded password PWi and the password entered from the input section 23 are collated by the collating section 22 (SB3), and informational use is forbidden when this collating result is an inequality (SB4). Moreover, when a collating result is coincidence, while decoding an encryption session key by common use encryption / decode section 27 using said card private key Ki (SB5), the information body enciphered using the session key obtained by this is decoded by common use encryption / decode section 27 (SB6), and the compounded information body is outputted from the information output section 29 (SB7).
[0035] In the above procedure, in case a terminal unit 2 receives information from information centre equipment 3, by not performing collating of a password to a positive, but collating a user identification number with a terminal unit 2, and collating a session key with information centre equipment 3, password collating is carried out tacitly as a result, and the user is attested.
[0036] Next, the operations sequence of the 2nd example at the time of receiving information is explained to a terminal unit 2 based on the flow chart of drawing 8 from information centre equipment 3. Here, the 2nd example is the approach of collating a password by the terminal unit 2 side.
[0037] Under the present circumstances, Password Ei (PEi) and the user verification key Ei which were enciphered with a registered user's user identification number UIDi and user verification key are accumulated in the user information storage section 31 of information centre equipment 3 as shown in drawing 9 .
[0038] First, it connects with information centre equipment 3 through the communications control section 20, the user identification number UIDi extracted from the security information are recording section 11 in the card section 1 is transmitted to information centre equipment 3, and a terminal unit 2 requires digital information (SC1).
[0039] The encryption password Ei (PWi) corresponding to said received user identification number UIDi is searched with information centre

equipment 3 from the user information storage section 31 (SC2). Subsequently, after the session key generation section 33 generates a session key (SC3) and verifying a session key using the user verification key Ei by the verification section 36 (SC4), it sets in the signature generation section 34. The following (8) As shown in a formula, it signs using the signature key Cs extracted from the center signature key are recording section 32 to said user identification number, an encryption password, and an encryption SESSHO key (SC5), and transmits to a terminal unit 2 (SC6).

[Equation 8]



Then, with a terminal unit 2, it is the following (9). As shown in a formula, said received signature information is verified in the verification section 21 with the center verification key Cp extracted from the security information are recording section 11 in the card section 1, a user identification number is taken out (SC7), and an encryption password is further signed with the user signature key Di in the signature generation section 26 (SC8).

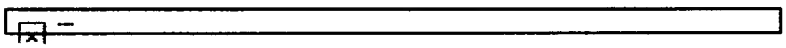
[0040]

[Equation 9]

Next, a terminal unit 2 compares the password entered as said transmitted user identification number, respectively (SC9), and as a result of this comparison, when either is an inequality, a circuit with information centre equipment 3 is cut (SC10). Moreover, the following (10) after a user identification number and a password sign said received encryption session key with a user signature key in coincidence (SC11) As shown in a formula, by the open encryption section 26, this signature information is enciphered with the center verification key Cp (SC12), and it transmits to information centre equipment 3 (SC13).

[0041]

[Equation 10]



In addition, since the processing of SC14-SC22 after this (even information centre equipment 3 session key collating, information body delivery, the are recording procedure to a terminal unit) is the same as that of the procedure of SA14-SA22 in the 1st example explained previously, the explanation is omitted.